Manipulation of Ideals

1. Radical ideals
   - the radical ideal membership problem

2. Independence Varieties
   - a problem in algebraic statistics

3. Zariski closure and Intersection of Ideals
   - Zariski closure
   - computing the generators of the intersection

4. Quotient of Ideals
   - computing a basis for the quotient and saturation
Manipulation of Ideals

1. Radical ideals
   - the radical ideal membership problem

2. Independence Varieties
   - a problem in algebraic statistics

3. Zariski closure and Intersection of Ideals
   - Zariski closure
   - computing the generators of the intersection

4. Quotient of Ideals
   - computing a basis for the quotient and saturation
polynomial ideals

An ideal $I$ generated by $N$ polynomials

$$f_i \in \mathbb{K}[x_1, x_2, \ldots, x_n] = \mathbb{K}[x], \ i = 1, 2, \ldots, N,$$

where $\mathbb{K}$ is an algebraically closed field, is defined as

$$I = \langle f_1, f_2, \ldots, f_N \rangle = \{ a_1 f_1 + a_2 f_2 + \cdots + a_N f_N \mid a_i \in \mathbb{K}[x] \}.$$

The variables involved in the polynomial ring matter.

An ideal $I$ in $\mathbb{K}[x]$ is not an ideal in $\mathbb{K}[x, y]$ because it is not closed under multiplication with variables in $y$.

Introducing a new variable is a useful technique, for example to solve the radical ideal membership problem.
radical of an ideal

For any ideal $I$, its radical is

$$\sqrt{I} = \{ p \in K[x] \mid p^k \in I \text{ for some } k \in \mathbb{N} \}.$$

One motivation for Gröbner bases is to solve the ideal membership problem, to decide whether $f \in I$.

The radical ideal membership problem: $f \in \sqrt{I}$.

For $I = \sqrt{I}$, we solve the ideal membership problem via the division (or normal form) algorithm if we have a Gröbner basis for the ideal.
Theorem 1 (radical ideal membership)

For \( I = \langle f_1, f_2, \ldots, f_N \rangle \) an ideal in \( \mathbb{K}[x] \) and \( f \in \mathbb{K}[x] \):

\[
f \in \sqrt{I} \iff 1 \in J := \langle f_1, f_2, \ldots, f_N, 1 - yf \rangle.
\]

Proof. To show the \( \Rightarrow \) direction, we have \( f \in \sqrt{I} \): there is a power \( k \geq 1: f^k \in I \).

As \( I \subset J: f^k \in J \).

We use \( k \) to show that \( 1 \in J \):

\[
1 = 1 - y^k f^k + y^k f^k = (1 - yf)(1 + yf + \cdots + y^{k-1} f^{k-1}) + y^k f^k \in J
\]

\( \in \) \( J \).
proof continued

For the $\iff$ direction, we have $1 \in J$:

$$1 = \sum_{i=1}^{N} p_i(x, y)f_i(x) + b(x, y)(1 - yf(x)), \quad y = 1/f$$

$$= \sum_{i=1}^{N} p_i(x, 1/f)f_i(x).$$

To clear all denominators of $p_i(x, 1/f)$, use a power $k$ of $f$.

Denoting the polynomials with cleared denominators as $P_i(x)$:

$$f^k = \sum_{i=1}^{N} P_i(x)f_i(x).$$

Thus $f \in \sqrt{I}$. \qed
To verify that an ideal is radical, we use the following

**Proposition 1**

Let $I$ be an ideal and $<$ be any term order. If the initial monomial ideal $\text{in}_<(I)$ is square free, then $I$ is a radical ideal.

One definition of a Gröbner basis $G$ is that $\text{in}_<(G)$ generates the initial ideal $\text{in}_<(I)$ so if all polynomials $g \in G$ are square free, then $I$ is radical. So a Gröbner basis provides an effective version of the proposition.
Manipulation of Ideals

1. Radical ideals
   - the radical ideal membership problem

2. Independence Varieties
   - a problem in algebraic statistics

3. Zariski closure and Intersection of Ideals
   - Zariski closure
   - computing the generators of the intersection

4. Quotient of Ideals
   - computing a basis for the quotient and saturation
We consider a conditional independence statement:

\[ A \perp B \mid C \] meaning: \( A \) is independent of \( B \) given \( C \).

An independence statement translates into a set of quadratic polynomials. We illustrate this with \( A \perp B \mid C \).

Suppose that \( A, B, \) and \( C \) are discrete random variables with outcomes in \( \{0, 1\} \). The statement

\[
\text{for all } i, j, k \in \{0, 1\} : \text{Prob}(A = i, B = j|C = k) = \text{Prob}(A = i|C = k) \times \text{Prob}(B = j|C = k)
\]

says that the probability of \( A = i \) and \( B = j \), given \( C = k \), is the product of the probabilities that \( A \) and \( B \) separately equal \( i \) and \( j \) respectively, given \( C = k \).

This probability statement expresses \( A \perp B \mid C \).
Deriving Equations

Denoting $p_{ijk} = \text{Prob}(A = i, B = j, C = k)$, for $i, j, k \in \{0, 1\}$ introduces eight indeterminates.

Via $\text{Prob}(A = i|C = k) = \text{Prob}(A = i, C = k)/\text{Prob}(C = k)$ we remove the conditional probabilities.

The statement $A$ is independent of $B$ given $C$ gives rise to the prime ideal

$$I_{A \perp B|C} = \langle p_{000}p_{011} - p_{001}p_{010}, p_{100}p_{111} - p_{101}p_{110} \rangle.$$  

Its variety $V(I_{A \perp B|C})$ is an independence variety.

The generators of $I_{A \perp B|C}$ are 2-by-2 minors of

$$\begin{bmatrix} p_{000} & p_{010} & p_{100} & p_{110} \\ p_{001} & p_{011} & p_{101} & p_{111} \end{bmatrix}.$$
Manipulation of Ideals

1. Radical ideals
   - the radical ideal membership problem

2. Independence Varieties
   - a problem in algebraic statistics

3. Zariski closure and Intersection of Ideals
   - Zariski closure
   - computing the generators of the intersection

4. Quotient of Ideals
   - computing a basis for the quotient and saturation
Zariski closure

Given an ideal $I = \langle f_1, f_2, \ldots, f_N \rangle$ of $\mathbb{K}[x]$ and we consider $V = V(I)$ as the solution set of the system $f(x) = 0$, defined by the polynomials $f_i$, $i = 1, 2, \ldots, N$.

In reverse, we consider as given a set $S \subset \mathbb{K}^n$ and consider

$$ I(S) = \{ f \in \mathbb{K}[x] \mid f(z) = 0 \text{ for all } z \in S \}. $$

For a set $S$, we define $\overline{S} = V(I(S))$ as the Zariski closure of $S$. $\overline{S}$ is the smallest variety that contains $S$.

**Proposition 2**

*For $S \subset \mathbb{K}^n$, $V(I(S))$ is the smallest variety that contains $S$.***

Note that for $W \supset S$: $I(W) \subset I(S)$ and $I(S)$ is a radical ideal.
elimination ideals

Elimination ideals are natural examples:

**Theorem 2**

Let \( I = \langle f_1, f_2, \ldots, f_N \rangle \) be an ideal in \( \mathbb{K}[x] \) with solution set \( V = V(I) \). Let \( \pi_\ell : \mathbb{K}^n \to \mathbb{K}^{n-\ell} \) be the projection onto the last \( n - \ell \) components. Let \( I_\ell = I \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n] \) be the \( \ell \)th elimination ideal. Then \( V(I_\ell) \) is the Zariski closure of \( \pi_\ell(V) \).

A Gröbner basis with a lexicographical term order provides a basis for the elimination ideal.
Manipulation of Ideals

1. Radical ideals
   - the radical ideal membership problem

2. Independence Varieties
   - a problem in algebraic statistics

3. Zariski closure and Intersection of Ideals
   - Zariski closure
   - computing the generators of the intersection

4. Quotient of Ideals
   - computing a basis for the quotient and saturation
Given two ideals $I$ and $J$ in $\mathbb{K}[x]$, we define their sum, product and intersection respectively as

$$I + J = \{ f + g \mid f \in I \text{ and } g \in J \}$$

$$I \cdot J = \langle \{ f \cdot g \mid f \in I \text{ and } g \in J \} \rangle$$

$$I \cap J = \{ f \in \mathbb{K}[x] \mid f \in I \text{ and } f \in J \}.$$

We leave it as an exercise to show that $I + J$, $I \cdot J$, and $I \cap J$ are ideals in $\mathbb{K}[x]$. 
examples

Good examples are monomial ideals.

For example, consider $I = \langle x^2 y \rangle$.
It is not too hard to see – think about the staircase representation of monomial ideals – that $I = \langle x^2 \rangle \cap \langle y \rangle$.

For $J = \langle xy^2 \rangle$, $I \cdot J = \langle x^2 y, xy^2 \rangle$ and $I \cap J = \langle x^2 y^2 \rangle$.

For general exponents $a, b \in \mathbb{N}^n$: $\langle x^a \rangle \cap \langle x^b \rangle = \langle x^c \rangle$, where $c$ is the least common multiple of $a$ and $b$. 
Given generators for $I$ and $J$, we consider the problem of computing generators for $I \cap J$.

**Theorem 3**

For $I$ and $J$ ideals in $\mathbb{K}[x]$: 

$$I \cap J = (tI + (1 - t)J) \cap \mathbb{K}[x].$$

**Proof.** We show the equality $=$ via containments $\subseteq$ and $\supseteq$.

$\subseteq$: $f \in I \cap J$ implies $f \in I$ and $f \in J$ and thus also $tf \in tI$ and $(1 - t)f \in (1 - t)J$.

Thus we can write $f$ as $f = tf + (1 - t)f \in tf + (1 - t)J$. Since $I$ and $J$ are ideals in $\mathbb{K}[x]$, we have $f \in (tI + (1 - t)J) \cap \mathbb{K}[x]$. 

Analytic Symbolic Computation (MCS 563) Manipulation of Ideals
\[ \forall f \in (tl + (1 - t)J) \cap \mathbb{K}[x] \text{ implies } f(x) = g(x, t) + h(x, t), \text{ for } g \in tl \text{ and } h \in (1 - t)J. \]

We show that \( f \in J \) by setting \( t = 0 \).

Because every element in \( tl \) is a multiple of \( t \): \( g(x, 0) = 0 \) and therefore: \( f(x) = h(x, 0) \).

Now we have to show that \( h(x, 0) \in J \).

Let \( J = \langle j_1, j_2, \ldots, j_N \rangle \), then for any \( h \in (1 - t)J \):
\[
h(x, t) = (1 - t)(a_1(x)j_1(x) + a_2(x)j_2(x) + \cdots + a_N(x)j_N(x)), \text{ for } a_i \in \mathbb{K}[x].
\]
As \( h(x, 0) = a_1(x)j_1(x) + a_2(x)j_2(x) + \cdots + a_N(x)j_N(x) \in J \), we have \( f \in J \).

Similarly, we can show that \( f \in I \) by setting \( t = 1 \).

Thus \( f \in I \cap J \).
The importance of the theorem is that it leads to an algorithm to compute the generators of \( I \cap J \).

Let \( I = \langle i_1, i_2, \ldots, i_r \rangle \) and \( J = \langle j_1, j_2, \ldots, j_s \rangle \) be ideals in \( \mathbb{K}[\mathbf{x}] \).

Then consider

\[
K = \langle ti_1, ti_2, \ldots, ti_r, (1 - t)j_1, (1 - t)j_2, \ldots, (1 - t)j_s \rangle \subset \mathbb{K}[\mathbf{x}, t].
\]

A Gröbner basis of \( K \) with respect to any lexicographical order for which \( t \) is greater than any variable in \( \mathbf{x} \) will give a Gröbner basis for \( I \cap J \).
In Macaulay 2, the command to intersect ideals is `intersect`.

From the documentation, we copy the input statements:

```plaintext
i1 : R = QQ[a..d];
i2 : intersect(ideal(a,b),ideal(c*d,a*b),
         ideal(b*d,a*c))
o3 = ideal (b*c*d, a*c*d, a*b*d, a*b*c)
```
solution set of $I \cap J$

The intersection turns into a union.

**Theorem 4**

For $I$ and $J$ ideals in $\mathbb{K}[x]$: $V(I \cap J) = V(I) \cup V(J)$.

**Proof.** We prove $= \subseteq$ in 2 steps: first $\subseteq$ and then $\supseteq$.

$$z \in V(I) \cup V(J) \Rightarrow z \in V(I) \text{ or } z \in V(J)$$

$$\Rightarrow f(z), f \in I \text{ or } f(z), f \in J$$

So for $f \in I \cap J$: $f(z) = 0$, thus $V(I) \cup V(J) \subseteq V(I \cap J)$.

For $\supseteq$, observe $V(I \cdot J) = V(I) \cup V(J)$.

We show $I \cdot J \subseteq I \cap J$. For $f \in I \cdot J$: $f = gh$, $g \in I$ and $h \in J$. Because $I$ is an ideal, $g \in I$ and $h \in \mathbb{K}[x]$ implies $gh = f \in I$. Likewise, because $J$ is an ideal, $f \in J$, so we have $f \in I \cap J$.

As $I \cdot J \subseteq I \cap J \Rightarrow V(I \cdot J) \supseteq V(I \cap J)$, the $\supseteq$ follows.
Manipulation of Ideals

1. Radical ideals
   - the radical ideal membership problem

2. Independence Varieties
   - a problem in algebraic statistics

3. Zariski closure and Intersection of Ideals
   - Zariski closure
   - computing the generators of the intersection

4. Quotient of Ideals
   - computing a basis for the quotient and saturation
ideal quotient

Let $I$ and $J$ be ideals in $\mathbb{K}[x]$, the ideal quotient of $I$ and $J$ (or colon ideal) is

$$I : J = \{ f \in \mathbb{K}[x] : fg \in I \text{ for all } g \in J \}.$$

We leave it as an exercise that $I : J$ is an ideal in $\mathbb{K}[x]$ and that $I \subseteq I : J$.

An example with monomial ideals justifies the name quotient:

$$\langle xz, yz \rangle : \langle z \rangle$$

$$= \{ f \in \mathbb{K}[x, y, z] : f \cdot z \in \langle xz, yz \rangle \},$$

$$= \{ f \in \mathbb{K}[x, y, z] : f \cdot z = a_1 xz + a_2 yz, \ a_1, a_2 \in \mathbb{K}[x, y, z] \},$$

$$= \{ f \in \mathbb{K}[x, y, z] : f = a_1 x + a_2 y, \ a_1, a_2 \in \mathbb{K}[x, y, z] \},$$

$$= \langle x, y \rangle.$$
The quotient $I : J$ can be computed via the intersection of quotient of $I$ with the generators of $J$, formally denoted as

$$I : \langle f_1, f_2, \ldots, f_N \rangle = \bigcap_{i=1}^{N} (I : f_i).$$

To justify this formula, we need to show that $I : (J + K) = I : J \cap I : K$ for ideals $I$, $J$, and $K$. 

using generators
Theorem 4

Let $I$ be an ideal in $K[x]$ and $f \in K[x]$. If $\{g_1, g_2, \ldots, g_s\}$ is a basis of $I \cap \langle f \rangle$, then $\{g_1/f, g_2/f, \ldots, g_s/f\}$ is a basis of $I : \langle f \rangle$.

Proof. We first show that any element in $\langle \frac{g_1}{f}, \frac{g_2}{f}, \ldots, \frac{g_s}{f} \rangle$ belongs to $I : \langle f \rangle$. We have:

$q \in \langle \frac{g_1}{f}, \frac{g_2}{f}, \ldots, \frac{g_s}{f} \rangle \Rightarrow fq \in \langle g_1, g_2, \ldots, g_s \rangle = I \cap \langle f \rangle$.

Applying $I : \langle f \rangle = \{ a \in K[x] \mid ap \in I, \text{ for all } p \in \langle f \rangle \}$. For $q$ to belong in $I : \langle f \rangle$, we must have that $qp \in I$ for all $p \in \langle f \rangle$. As $p \in \langle f \rangle$, $p = bf$, for some $b \in K[x]$. So $qp = qbf$ and $q \in I \cap \langle f \rangle \subset I$. Thus $q \in I : \langle f \rangle$. 
We still have to show that every \( q \in I : \langle f \rangle \) is a polynomial combination of \( \left\{ \frac{g_1}{f}, \frac{g_2}{f}, \ldots, \frac{g_s}{f} \right\} \).

For \( q \in I : \langle f \rangle \), we have: \( fq \in I \).

Since \( fq \in \langle f \rangle \), we have \( fq \in I \cap \langle f \rangle \), so \( fq = a_1g_1 + a_2g_2 + \cdots + a_sg_s \), for \( a_i \in K[x], \ i = 1, 2, \ldots, s \), as \( \langle g_1, g_2, \ldots, g_s \rangle = I \cap \langle f \rangle \).

Because each \( g_i \in \langle f \rangle \), each \( g_i/f \) is a polynomial, and we have
\[
q = a_1 \frac{g_1}{f} + a_2 \frac{g_2}{f} + \cdots + a_s \frac{g_s}{f}.
\]

The theorem gives an algorithm to compute \( I : J \) for \( J = \langle j_1, j_2, \ldots, j_s \rangle \), using \( I : \langle j_1, j_2, \ldots, j_s \rangle = \bigcap_{i=1}^{s} (I : j_i) \).

\[ \square \]
In Macaulay 2, copying from the online documentation, we compute the quotient of two ideals via the colon operator (the command quotient allows the user to give options):

```
i1 : R = QQ[a..d];
i2 : I = ideal(a^2*b-c^2,a*b^2-d^3,c^5-d);
i3 : J = ideal(a^2,b^2,c^2,d^2);
i4 : I:J
     2 3 2 2 5
o4 = ideal (a*b - d, a*b - c, c - d)
```
The saturation of \( I \) by \( p \) is

\[
(l : p^\infty) = \{ q \in \mathbb{K}[x] \mid qp^N \in I, \text{ for some } N \}.
\]

Geometrically, the components of \( V(l : p^\infty) \) are those components of \( V(l) \) which do not lie on the hypersurface \( p^{-1}(0) \).

Via Gröbner bases we may compute \((l : p^\infty)\) as follows. Let

\[
J = l + (tp - 1) \in \mathbb{K}[t, x], \quad \text{then} \quad (l : p^\infty) = J \cap \mathbb{K}[x].
\]

Gröbner bases with a lexicographical term order eliminate.

The Macaulay 2 command for saturation is \texttt{saturate}. 
### Algebra ↔ Geometry

<table>
<thead>
<tr>
<th><strong>Algebra</strong></th>
<th><strong>Geometry</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>radical ideal $I = \sqrt{I}$</td>
<td>$V(I)$ variety</td>
</tr>
<tr>
<td>$I(V)$ ideal of a set</td>
<td>solution set $V$</td>
</tr>
<tr>
<td>sum of ideals $I + J$</td>
<td>$V(I) \cap V(J)$ intersection of varieties</td>
</tr>
<tr>
<td>$\sqrt{I(V) + I(W)}$ radical of sum</td>
<td>intersection of sets $V \cap W$</td>
</tr>
<tr>
<td>product of ideals $IJ$</td>
<td>$V(I) \cup V(J)$ union of varieties</td>
</tr>
<tr>
<td>$\sqrt{I(V)I(W)}$ radical of product</td>
<td>union of sets $V \cup W$</td>
</tr>
<tr>
<td>intersection of ideals $I \cap J$</td>
<td>$V(I) \cup V(J)$ union of varieties</td>
</tr>
<tr>
<td>$I(V) \cap I(W)$</td>
<td>union of sets $V \cup W$</td>
</tr>
<tr>
<td>quotient of ideals $I : J$</td>
<td>$V(I) - V(J)$ difference of varieties</td>
</tr>
<tr>
<td>$I(V) : I(W)$</td>
<td>difference of sets $V - W$</td>
</tr>
<tr>
<td>elimination $\sqrt{I \cap \mathbb{C}[x_{k+1}, \ldots, x_n]}$</td>
<td>$\pi_k(V(I))$ projection of varieties</td>
</tr>
</tbody>
</table>
Gröbner bases provide algorithms to manipulate ideals.

Exercises:

1. For ideals $I$ and $J$ in $\mathbb{K}[x]$, show that $I + J$, $I \cdot J$ and $I \cap J$ are ideals in $\mathbb{K}[x]$.
2. For $I = J = \langle x, y \rangle$, show that $I \cdot J \subsetneq I \cap J$.
3. Let $I = \langle x_1x_4 + x_2x_3, x_1x_3, x_2x_4 \rangle$. Compute $(I : x_4^2)$.
4. Show that $V(I \cap J) = V(I) \cup V(J)$ for ideals $I$ and $J$ in $\mathbb{K}[x]$. 

Summary + Exercises